Statement of Subcommittee Chairman John Ratcliffe (R-TX)
Subcommittee on Cybersecurity and Infrastructure Protection

Joint Subcommittee Hearing:

"Public-Private Solutions to Educating a Cyber Workforce""

October 24, 2017

Remarks as Prepared

Let me begin by welcoming our witness panel and our guests today. Thank you for taking the time away from your important work to testify and help Congress better understand these workforce issues. I am especially grateful for the opportunity to collaborate with the Members of the Higher Education and Workforce Development Subcommittee to hold this joint hearing on developing our nation's cyber workforce. I would like to thank Chairwoman Foxx and Chairman Guthrie for their work on this critical issue. It is an important time for cooperation here on Capitol Hill and it is my sincere hope that the public will be encouraged that Members on both sides of the aisle are focused on important issues that really matter.

Cybersecurity is an issue that affects every sector of our economy and our society. The risks are broadly shared and this joint hearing shows the need for an integrated approach to address the challenge of the cyber skills gap. Cyber-attacks are growing in frequency and sophistication, but the availability of qualified cybersecurity professionals to deal with these challenges is not keeping pace. We cannot speak to the shortage of workers without recognizing the importance of the academic pipeline that produces today's workforce as well our next generation of experts who will need to keep pace with technology and the ever evolving threats.

The dearth of cybersecurity talent is a major resource constraint that impacts our ability to protect information and assets. More than 200,000 cybersecurity jobs in the U.S. are unfilled and the demand for positions, like information security professionals, is expected to grow by 53 percent through 2018. This slow moving crisis is very likely to only get worse.

The Cybersecurity and Infrastructure Protection subcommittee recently heard testimony that indicated that the struggle to find qualified personnel to fill cybersecurity roles in government and business is not only a short term problem, but is expected to grow and become even more acute in the future. Technology innovation and criminal tactics move very fast, and with each new wirelessly-connected baby monitor or interconnected energy-efficient pipeline that comes online, new threats and vulnerabilities emerge to exploit those technologies. Just as the connected world expands and new products improve our quality of life, simplifying many tasks, our vulnerabilities move in parallel and demand a skilled workforce who can protect the functionality and preserve confidential data.

Public and private hiring systems must likewise shift and adapt to a new way of thinking about hiring and recruiting; we need intellectual capital that better reflects the qualifications and skills of a new type of cyber worker. For their entire lives, younger Americans just entering the workforce have possessed more technology in a single smartphone than some ever imagined. Consider that the iPhone 7 operates at 1.4 gigahertz and can process instructions at a rate of approximately 1.2 instructions every cycle in each of its 2 cores. Put simply, the iPhone 7's clock is 32,600 times faster than the best Apollo-era computers and could perform instructions 120,000,000 times faster. You wouldn't be wrong in saying an iPhone could be used to guide 120,000,000 Apollo era spacecraft to the moon, all at the same time. The rate of innovation in the information technology sector is simply astonishing.

I believe the Federal Government and our cybersecurity leaders can create more alliances with community groups, universities and career and technical schools to better develop our talent pipeline. The Department of Homeland Security supports a number of efforts to strengthen its workforce, from programs to recruit new cyber talent to those that allow private sector experts the opportunity to share their knowledge working at DHS. We need to encourage government-university-employer collaborations that are meaningful and robust. Demonstrating cyber know-how no longer comes in discrete forms such as having a bachelor's degree or not, or obtaining a cyber certification. Cyber competitions, bug bounty programs, and coding camps are all new forms of workforce development

I am looking forward to discussing with our witnesses today some of the best practices in building public-private partnerships to expand the cyber workforce pipeline.

The cyber capabilities of our workforce help support economic strength and sustain our technological advantage. It is my firm belief that America will only remain the world's preeminent superpower so long as it remains the world's cybersecurity leader. Leadership matters, and if we don't encourage and develop the talented men and women who lead this work, we will be both poorer and less safe.

###